RFI SIEM Solution – Question & Answer 1

The VA does not show any data collection points at Martinsburg, WV and Hines, IL even though the central event collection systems exist at these two locations for systems that provide significant amounts of data. Is it VA's plan to move the central event collection systems to the 4 TIC gateways? Or should the proposed design include event collection capabilities at Martinsburg and Hines to minimize WAN traffic?

The 4 TIC gateways are the source and collection sites for most of the data monitored by the NSOC. However, NSOC managed devices at NSOC sites, including Hines and Martinsburg, will be sending logs to the SIEM in the nearest gateway.

The diagram provided from the VA shows event data going to both Hines and Martinsburg to the consoles. Does the VA expect that both Hines and Martinsburg can act as the primary console at any time or is this a depiction of what it should look like during a failover? As the VA likely knows, many SIEM solution cannot have 2 primary consoles serving data at the same time. Could this be amended if so to show this as a fail-over/DR scenario?

Both sites should be active with synchronization of rules, not event data, between the two. The primary console is located in Martinsburg, with Hines serving as an active standby/failover/DR system.

If proposed, would the VA consider SIEM as a Service? Meaning that the SIEM consoles and data were hosted for VA and only collection VM's we placed inside the VA to minimize cost and impact to the VA. This way the VA would only need to pay for the space and compute resources it used on a monthly basis. If the VA would like the data at the end of the terms, the VA would be inclined to take the data.

This question asks if "SIEM as a Service" solutions, which are related to other IaaS or Saas solutions, would be considered as a candidate offering. The vendor should propose a solution aligned against the requirements stated in the RFI. If the vendor interprets all of the requirements in a way that can be met using a SIEM as a Service solution, they should detail their offering accordingly.

The VA's training requirement shows the need for 2 basic and 1 advanced class per location (Martinsburg and Hines). This comes to a total of 120 users being trained. To verify, the VA would like pricing for training 120 users on the SIEM solution with 100 of them being basic users and 20 being advanced users?

The RFI states that a total of six (6) separate training sessions will be held, divided into three (3) sessions each at Martinsburg and Hines. Each site will have two (2) basic user training session and one (1) advanced user training session. The requirement is for up to ten (10) attendees per advanced user session and up to twenty five (25) attendees per basic user session. The requirement therefore needs to account for up to one hundred (100) basic user training attendees and up to twenty (20) advanced user training attendees.

The current diagram depicts NO storage associated with the Data Analysis Consoles, is this correct? This is a design change which could result in a 4X increase in storage at each TIC gateway location.

The VA recognizes the potential need for storage as part of the Consoles at the analysis sites (HITC & CRRC). The collection sites are to remain the primary storage location of all collected

data and be relied upon for satisfying the retention of data requirement. Therefore, data pulled to the analysis sites would not need to adhere to retention requirements. Vendors shall state the recommended storage configuration and account for all storage needs as part of their proposal. This may vary by solution and should be accounted for in the response.

Under the current design should storage be included for the one year retention and replication between the Console sites?
The RFI provides requirements for data retention and replication for 1 years in two different tiers. The VA recognizes the potential need for storage as part of the Consoles at the analysis sites (HITC & CRRC). The collection sites are to remain the primary storage location of all collected data and be relied upon for satisfying the retention of data requirement. Therefore, data pulled to the analysis sites would not need to adhere to retention requirements. The response should explain how their solution will meet these requirements and explain why it is an effective solution. Regarding replication between Hines and Martinsburg, both sites need to be effectively synchronized in such a way that either is operationally capable of being the primary console at all times.

In previous design submissions, our team has used physical Netflow collectors as the basis for determining capacity requirements. The current RFI has added virtual devices. Can VA provide the specifications for these virtual devices.
Virtual devices proposed shall be capable of processing data at volumes described in the RFI. The vendor will need to specify the number of CPUs, memory, disk IO throughput, etc… that they require for the solution, and should include and account for all hardware they need for data collection.

Requirement 5.4.1.5 in the draft PWS states, "The systems shall be able to process at a minimum 20,000 events per second per instance" but 5.4.1.9 states "The systems shall be able to immediately handle 60,000 events per second at each location. Proposed architecture without major modification shall be scalable to 120,000 events per second." Does the VA intend to have multiple instances per location, or a single instance per location capable of 60,000 events per second with the ability to increase licensing without modifying the architecture to 120,000 events per second?
Each logging device shall be capable of handling 20,000 events per second. Each TIC GW is expected to generate up to 60,000 events per second. The solution in each GW shall be scalable to handle 120,000 events per second.

The Test Acceptance Plan states that specific areas of testing focus will include "Integration with Splunk; Splunk and SIEM Solution performance…" As there are not specific requirements in the draft PWS pertaining to this integration, can you provide more detailed requirements for the Test Acceptance Plan?
Please see Attachment 3 Test Acceptance Plan SIEM revised 6 24 2014.

Could you please provide an extension until Friday 6/27?
The RFI due date and time has been extended from Wednesday, June 25, 2014 at 12 Noon EST to Monday, June 30, 2014 at 12 Noon EST.